

PAT-NO: JP410214183A
DOCUMENT-IDENTIFIER: JP 10214183 A
TITLE: COMPUTER BIOS UPDATING SYSTEM

PUBN-DATE: August 11, 1998

INVENTOR-INFORMATION:

NAME	COUNTRY
EDA, HIDEKI	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	N/A

APPL-NO: JP09032785

APPL-DATE: January 30, 1997

INT-CL (IPC): G06F009/06 , G06F009/06 , G06F012/16 , G06F013/00

ABSTRACT:

PROBLEM TO BE SOLVED: To improve the security by automatically limiting a specified operation and to improve the reliability by making risks small, by providing a machine identifier in an accessible register intrinsically provided in a server.

SOLUTION: A flash ROM 102 is provided with the function of electric erasure and write by a program and a BIOS program is stored in the flash ROM 102. A main memory 103 for system management is used as an area for storing data for server maintenance and used for the checking of machine ID(identifier) discrimination by the rewrite of BIOS and the preservation of a rewrite instruction request flag from a host terminal. Then, in the case that the machine ID is not correct, since normal BIOS write is not performed, the rewrite error of mistaking data or the like is prevented and safety is provided in terms of a user operation.

COPYRIGHT: (C)1998,JPO

【特許請求の範囲】

【請求項1】電気的に書き換え可能な不揮発メモリであるフラッシュROMに基本入出力制御システムのファームウェア情報であるBIOS (Basic Input/Output System) を備えたサーバ装置において、固有に持つアクセス可能なレジスタにマシン識別子を備えたことを特徴とするサーバ装置。

【請求項2】レビジョン情報と共に、リード/ライトにより前記フラッシュROMの正当性を判断する機能と、前記フラッシュROMの不具合を検知したとき、もしくは、前記BIOSの書き換えがホスト端末より指示されたときに、前記フラッシュROMの書き換えを実行する機能と、を備えたことを特徴とするBIOS。

【請求項3】前記BIOSの書き換え機能判別を含む保守情報を格納する不揮発性RAM (「NVRAM」という) を備えたことを特徴とする請求項1又は2記載のサーバ装置。

【請求項4】電気的に書き換え可能な不揮発メモリであるフラッシュROMに基本入出力制御システムのファームウェア情報であるBIOSを備えたサーバ装置のBIOSのアップデート方式において、システム起動時、前記フラッシュROMのデータをチェックすると共に、不揮発型ランダムアクセスメモリに書き込まれたマシン固有のID情報と、BIOSのレビジョン情報により、書換BIOSデータの正当性をチェックし、これらのチェックの結果が共に可の場合、前記フラッシュROMに格納されているBIOSを所定の記憶装置にバックアップした後に、前記フラッシュROMを消去し、BIOSの書き換えを実行する、ことを特徴とするBIOSのアップデート方式。

【請求項5】前記フラッシュROMのBIOSをバックアップした後の検証において、検証結果が不可の場合、予め定められた所定のキーが押下された時、強制的に前記フラッシュROMのBIOSの書き換えを実行する、ことを特徴とする請求項4記載のBIOSのアップデート方式。

【請求項6】前記フラッシュROMの消去の検証において、消去結果が不可の場合、前記フラッシュROMデータのチェックを行い、その結果が不良の場合には、前記バックアップされたBIOSデータにより前記フラッシュROMのBIOSの書き換えを実行する、ことを特徴とする請求項4記載のBIOSのアップデート方式。

【請求項7】前記フラッシュROMにおいて、システム起動時に実行するブートブロックを残して書き換えを実行する、ことを特徴とする請求項4記載のBIOSのアップデート方式。

【請求項8】前記フラッシュROMの前記ブートブロックに、前記フラッシュROMのデータの整合性をチェックする手段と、前記フラッシュROMの書き換え不具合

検出時にリカバリ処理を行う手段と、を備えたことを特徴とする請求項4記載のBIOSのアップデート方式。

【請求項9】請求項2記載のBIOSのコードを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータサーバ装置に関し、特に、システムの基本入出力装置であるBIOS (Basic Input/Output System; オペレーティングシステム中で周辺装置等ハードウェアに依存する制御プログラム) が格納される、電気的に書き換え可能なフラッシュROMを有し、また、書き換えのためのデータを格納するデータ記憶装置を持ち、システムのバージョンアップ時や不具合が検出された時に迅速な対応と堅実的で信頼性の求められるサーバ装置に関する。

【0002】

【従来の技術】従来、コンピュータシステムの分野では、電源投入時や、システムリセット時における起動時の初期設定、システムコンディションチェック、および基本入出力制御のためのファームウェアであるBIOSが、デバイス増設に伴うシステム状態の変更や、バグ/不具合吸収、もしくはBIOS自身の機能向上のために、「フラッシュROM」と称される電気的に書き換え可能なROM (リードオンリメモリ) で提供されていることが、一般的となってきた。

【0003】このBIOSの書き換えに関して、書き換えデータおよび、書き換えツールを入手すれば、技術的にはユーザが自ら行うことも可能である。

【0004】しかしながら、技術的な情報不足、あるいは単純な手順ミスなどの人為エラーから、BIOS書き換え後にシステムそのものが立ち上がらなくなる可能性を含み、また操作ミス以外の事故、例えばBIOS書き換え中の停電の発生などでも、システムの起動が不可能になるという事態が起こり得る、ことになる。

【0005】さらに、急速なコンピュータ分野の発達により、BIOS書き換えは、将来的には、通常のアプリケーションを使うように、ユーザが自ら行える保守の範疇に入ることも想定されるが、前述したような、僅かなミスで、システムの起動が不可能になってしまうのではリスクが余りに大きすぎ、このためユーザにBIOSを提供することはサポートの点を考えると、實際上、困難である。

【0006】特に、クライアント・サーバ方式におけるサーバシステムのような安全性を重視する企業等の基幹システムにおいては、迅速なシステムアップ、及び不具合の修正等の対応が求められるが、現在は、開発側と、一部のシステムをよく理解している保守員のみを利用されているにすぎない。

【0007】なお、例えば特開平5-73441号公報には、BIOSメモリとしてフラッシュEEPROM

(Electrically Erasable and Programmable ROM)を使用した場合にメモリ内容を保証して安全に書き込みができる機構を備えたパーソナルコンピュータの構成が提案されている。

【0008】

【発明が解決しようとする課題】以上説明したように、上記した従来方式は下記記載の問題点を有している。

【0009】(1)第1の問題点は、上記のように、BIOSの書き換え動作には、安全性が重視されるが、前述したような僅かのミスでシステムが起動不可能になってしまうという可能性があり、信頼性に重きを置くサーバシステムとしては、著しく問題がある、ということである。すなわち、上記のようなシステム起動不可等の障害が原因して、例えば企業内システムがストップしてしまうという可能性すらある。

【0010】また、現在のBIOS書き換え手順は、ユーザサイドから見ると、制限が多く、正しく書き換えツールを運用することはほとんどできない、ものと考えられる。このため、現状では、ユーザサイドでのBIOS書き換えを推奨することはできず、保守員が現地に出向いたり、PKG(パッケージ)交換をして、工場で処理するなど、時間と労力を多大に費やすことになるだけでなく、信頼性をも大きく損なう場合もある。

【0011】その理由は、運用方法がわかりにくく、BIOSの書き換えツールの使用方法に、装置固有の限定条件などが付帯している、ためである。

【0012】(2)第2の問題点は、何らかのミス、障害等で偶然BIOSの書き換えが失敗したとしても、システムそのものが立ち上がらなくなることには変わりなく、失敗した場合のリスクが大きすぎることである。

【0013】その理由は、誰もが簡単に操作可能なリカバリ手段(復旧手段)が提供されていない、ためである。

【0014】したがって、本発明は、上記問題点により鑑みてなされたものであって、その目的は、特定の動作を自動で制限することによりセキュリティを向上し、同様の理由で、リスクを極力小さくすることにより、信頼性を向上するシステムを提供することにある。本発明の他の目的は、自動運用を可能とすることにより操作を簡易なものとし、リカバリ手段を提供することで現場での対応が可能となり、保守および信頼性、また操作性が向上するシステムを提供することにある。

【0015】

【課題を解決するための手段】前記目的を達成するため、本発明は、電氣的に書き換え可能な不揮発メモリであるフラッシュROMに基本入出力制御システムのファームウェア情報であるBIOSを備えたサーバ装置において、前記サーバ装置が固有に持つアクセス可能なレジスタにマシン識別子を備えたことを特徴とする。

【0016】また、本発明においては、BIOSが、レ

ビジョン情報と共に、リード/ライトにより前記フラッシュROMの正当性を判断する機能と、前記フラッシュROMの不具合を検知したとき、もしくは、前記BIOSの書き換えがホスト端末より指示されたときに、前記フラッシュROMの書き換えを実行する機能と、を備えたことを特徴とする。

【0017】

【発明の実施の形態】本発明の好ましい実施の形態について以下に説明する。本発明は、その好ましい実施の形態において、サーバコンピュータにおけるBIOS書き換え機能は、自動でシステムを判断し、必要な手続きを発行して書き換えを実行する。その際、不慮の事故を考慮に入れて、書き換え実行が正常に実行されたかを検出する機能手段と、正常に実行されなかった場合のリカバリ機能手段を提供する。

【0018】より具体的には、本発明の実施の形態においては、サーバ装置に、それぞれモデルごとに一意のマシンIDをシステムの保守機能用に提供されるNVRAM(不揮発性ランダムアクセスメモリ)の任意のエリアに与えることにより、マシン判別を容易にするとともに、BIOS書き換え動作の自動実行手順を定義することにより、ユーザの手をわずらわせない簡易な書き換え動作を可能とする。

【0019】また、その際、ホスト端末(例えば保守センタ)からの書き換え要求により、直接、対象端末側にいなくても、BIOSの書き換え実行が可能である。

【0020】また書き換えに際しては、フラッシュROM、すなわち一括消去型EEPROM(電氣的に消去及び書き換え可能な読み出し専用メモリ)の特定のエリアを保護し、書き換えない部分として固定する。

【0021】この部分には、システム起動時に、フラッシュROMのチェックサム(Checksum)からの正当性を判断し、チェックサムに問題があれば、書き換え時に、バックアップしたBIOSデータで書き戻しを試みる。

【0022】またBIOS書き戻し指示が失敗した場合、リモートで保守センタに連絡が行くようなプログラムが組まれている。

【0023】さらに現地調査で保守員が特定のキーをキーボードから押下しているのを検知して、フロッピーディスク(FD)からのデータロードによるBIOS書き換えが動作する。

【0024】本発明の実施の形態においては、サーバコンピュータのフラッシュROMを、システム起動時に実行するブートブロックを残して書き換え実行することで、ROMのアクセス範囲制御のための回路を取り除くことができる。

【0025】このとき、BIOSデータのバックアップを内蔵する記憶装置内にバックアップしておくので、このブートブロックに、フラッシュROMの整合性チェック手段を与えることで、フラッシュROMの書き換え不

具合を立ち上げ時に検出し、同じくブートブロック内にあるリカバリ機能の提供によって、BIOS書き戻し手段が実行され、万が一、BIOSのアップデートに失敗した時にも対応できる。

【0026】またキー入力検出手段のキー入力の判定により、書き換えデータに問題があった場合でもFD媒体供給による正しいデータを即時強制的に適用できる機能を有する。このため、バックアップデータが不正であっても保守員が障害通報からすぐに回避手段をとることができる。

【0027】本発明の実施の形態においては、このようにして、障害対策を早期に手軽に行うことが可能である。

【0028】

【実施例】上記した本発明の実施の形態について更に詳細に説明すべく、本発明の実施例について図面を参照して以下に説明する。

【0029】図1は、本発明の一実施例に係るサーバコンピュータの構成を示すブロック図である。図1を参照すると、本実施例において、サーバコンピュータは、プロセッサ101と、BIOSを格納するフラッシュROM（一括消去型EEPROM）102と、システム保守情報を格納するシステム管理用NVRAM（Non Volatile RAM；不揮発性ランダムアクセスメモリ、図中メインメモリで示す）103と、入力装置105と、表示装置104と、データ記憶装置106と、を備えて構成されている。これらは、いずれもバス100に接続されている。

【0030】フラッシュROM102は、プログラムにより電気的消去及び書き込みの機能を備えており、BIOSプログラムは、このフラッシュROM102に格納されている。

【0031】システム管理用NVRAM103は、RAS機能を持つシステムに提供されるNVRAMを、サーバ保守用のデータが格納される領域として使用し、本実施例では、BIOSの書き換えによるマシンID（識別子）判別のチェック用、および、ホスト端末からの書き換え指示要求フラグの保存に使用される。

【0032】図2は、本実施例の処理フローを説明するためのフローチャートである。図1及び図2を参照して、本実施例の動作について以下に説明する。

【0033】電源ONによるシステム起動時、BIOSは、ブートブロックといわれるライトプロテクトされた領域から実行する。ブートブロック内の判定部01（フラッシュROMチェックサムルーチン）は、フラッシュROM102へBIOSを格納したときに同時に書き込まれているチェックサムと、起動時にとったチェックサムと、を比較し、フラッシュROM102内のBIOSデータの整合性を確認する（ステップS1）。

【0034】不整合であれば、自動リカバリ処理とし

て、データ記憶装置106に格納してあるBIOSデータを使って、実行部13よりBIOS書き込みを試みる（ステップS9）。

【0035】ステップS1において、チェックサムが正しい場合には、BIOSは、ブートブロックから判定部02（キー押下及び書き換え指示制御フラグチェックルーチン）を実行し、強制的にBIOS書き換えを実行するかどうかを入力装置105におけるキー押下チェック、もしくは保守用のシステム管理用NVRAM103に設ける書き換え指示制御フラグより判断し（ステップS2）、強制BIOS書き換えキー押下時、もしくはOS（オペレーティングシステム）上から書き換え要求コマンドが実行されたとき、データ記憶装置106からBIOSデータを使用して実行部13よりBIOS書き換えを実行を試みる（ステップS9）。

【0036】強制キー押下を検出しない、もしくは、書き換え指示制御フラグがOFFだった場合、BIOSは、実行部11にて、システム管理用NVRAM103内にある、マシンID領域に、マシンIDとBIOSレビジョンを格納する。

【0037】このマシンIDは、BIOS書き換え時における書き換えプログラムのシステム判別に使用される。

【0038】そして、このマシンIDが正しくない場合、通常のBIOS書き込みは行われないので、データを間違える等の書き換えミスを防ぐことが可能になり、ユーザ運用上も安全になる。

【0039】また、このマシンIDは、将来のシステムアップ時に、システムアップしていない他のモデルと差別化をはかるため、マシンID部分のみの書き換えインターフェース機能も提供される。

【0040】さらに、本実施例においては、BIOSレビジョン（Revision）も、BIOS書き換え時に、参照されるもので、このBIOSレビジョンのチェックにより、無用なデグレードを防ぐ。

【0041】マシンID書き込み後、BIOSの通常のPOST（試験診断；電源オン時の自己試験）処理を実行し、起動する。

【0042】起動時、システムは、フロッピーディスク（FD）記録媒体が、フロッピーディスクドライブ装置に挿入されていれば、フロッピーディスクからブート（boot）する（ステップS4）。

【0043】このフロッピーディスク（FD）が、BIOS書き換え用ツール実行媒体なら、書き換えツールは、判定部03以下のBIOS書き換え処理を実行する。

【0044】判定部03にて、実行部11で、システム管理用NVRAM103に書き込まれたマシンIDと、FD内にある書き換えのために準備されたBIOSデータ内のマシンIDと、を比較し（ステップS5）、こ

らが互いに異なるようなら、実行部16により、表示装置105に用意された書き換えデータが正しいものではないので、書き換えを実行しない旨のエラーメッセージを表示し(ステップS17)、実行部15によりシステムを止める(ステップS18)。そして、リセットスイッチか電源スイッチ等による再起動(リブート)を待機する。

【0045】判定部03において、BIOSデータがこのサーバシステム固有のものであるものと判断されたら(ステップS5のOK分岐)、判定部04(BIOSレビジョンチェックルーチン)を実行する(ステップS6)。この判定部04では、BIOSレビジョンを確認し、書き換えのために準備されたデータが現行BIOSのレビジョンと同じか、これよりも古ければ、判定部03におけるNG(不良)の場合と同様、ステップS18に分岐し、エラー表示処理後、システムを止める。

【0046】判定部04でのチェックで、書き換えのために用意されたBIOSデータが新規のものであると判断されたら(ステップS6のOK分岐)、実行部12にて、データ記憶装置に現行BIOSのデータをファイルとして保存する(ステップS7)。

【0047】このBIOSのバックアップデータは、実行部12以後の書き換え処理で、書き換え途中で電源が落ちたなどの障害が発生し、次回立ち上げ時に、BIOS異常があった場合、例えば、フラッシュROM102に記憶されるデータのチェックサムが正しくないなどの場合に、BIOS書き戻し処理用のBIOSデータとして用いられる。

【0048】実行部12による現行BIOSのバックアップ完了後、バックアップBIOSデータのペリファイを実行し、判定部05のペリファイ結果にNG(不可)があった場合、実行部17により、バックアップデータに異常があること、処理続行するかを問うメッセージを表示装置104に表示し(ステップS14)、処理続行のためのキーが押されたら、判定部08で判断されれば、実行部15で終了メッセージを表示し(ステップS18)、システムを止め、再起動(リブート)を待機する。

【0049】判定部05において、バックアップBIOSデータのペリファイが正しいか(ステップS8のOK分岐)、判定部08において処理続行のキーが押下されたらと判断された場合(ステップS16のY分岐)、実行部13により、フラッシュROM102のブートブロック以外の領域を初期化する(ステップS9)。

【0050】実行部14において、フラッシュROMデータリードでフラッシュROM102の初期化が正常に行われたかを判断し(ステップS10)、正しく行われていなければ、実行部18にて、フラッシュROMの初期化に失敗したことを、エラーメッセージとして表示し(ステップS13)、判定部09により、ROMデータ

のチェックサムをとり(ステップS14)、その結果がNG(不良)ならば、バックアップされているBIOSデータを使ってBIOS書き換え実行し(ステップS19)、一方、OKならば、システムを止めて、再起動(リブート)を待機する(ステップS18)。

【0051】判定部06の結果より、フラッシュROM102の初期化が正常終了したら、フロッピーディスク(記録媒体)にファイルとして提供されている新規BIOSデータを用いて、実行部14によりフラッシュROM102にBIOS書き込み動作を実行する。

【0052】実行部14完了後、FD内の新規BIOSデータと、フラッシュROM102に書き込みされたBIOSデータのペリファイ処理を行い、判定部07よりBIOS書き込みが正常に行われたかを確認する(ステップS12)。この判定の結果、NG(不可)の場合、既にバックアップされているBIOSデータを用いて、実行部13でのBIOS書き戻し処理を試みる。

【0053】判定部07で、BIOS書き換えが正常終了したならば、実行部15より書き換え動作完了メッセージを表示し、システムを止め、再起動を待機する。

【0054】

【発明の効果】以上説明したように本発明は、下記記載の効果を奏する。

【0055】(1)本発明の第1の効果として、極力ユーザの手が介入しないBIOS書き換え処理を可能とし、操作ミスの発生する可能性を極力低減する、ということである。

【0056】(2)本発明の第2の効果は、保護チェック機能強化により、安全で確実なBIOS書き換え機能をユーザに提供できる、ということである。

【0057】(3)本発明の第3の効果は、簡易なリカバリ方法の提供により、万が一の不具合時にも、対応を容易化し、保守性を向上している、ということである。

【0058】(4)本発明の第4の効果は、簡易で、ほぼ完全な自動化により、BIOS書き換え時の作業効率を向上する、ということである。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示すブロック図である。

【図2】本発明の一実施例の処理フローを説明するための流れ図である。

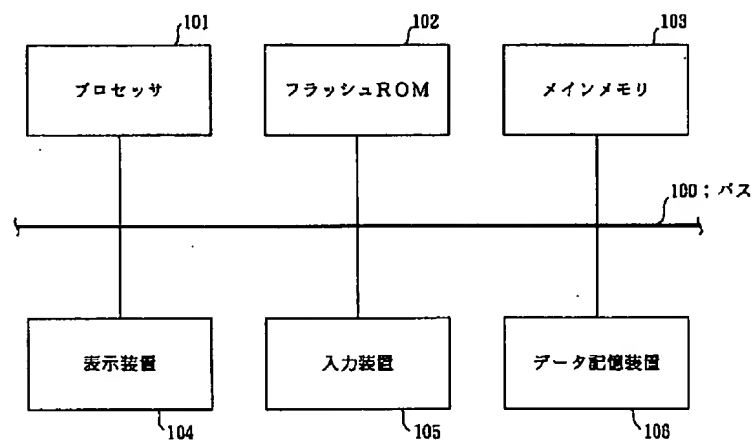
【符号の説明】

100 バス
101 プロセッサ
102 フラッシュROM
103 メインメモリ
104 表示装置
105 入力装置
106 データ記憶装置
S1 フラッシュROMチェックサムルーチン

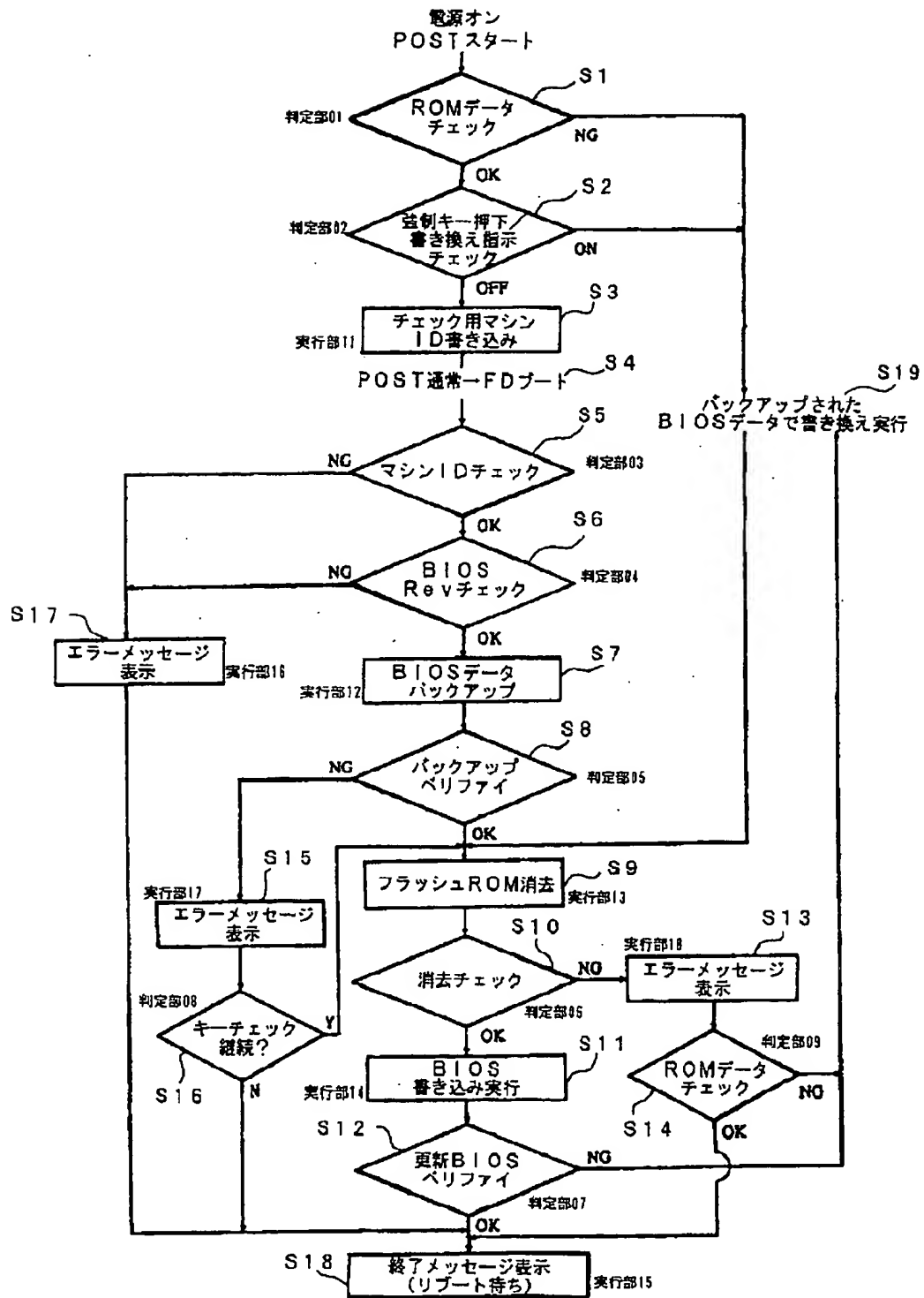
S2 キー押下及び書き換え指示制御フラグチェックルーチン
 S3 マシンID保守用NVRAMへの書き込み処理
 S5 マシンIDチェックルーチン
 S6 BIOSレビジョンチェックルーチン
 S7 BIOSデータバックアップ
 S8 バックアップBIOSデータベリファイチェックルーチン
 S9 フラッシュROM消去処理

S10 フラッシュROM消去チェックルーチン
 S11 BIOS書き込み処理
 S12 更新されたBIOSベリファイチェックルーチン
 S13、S15、S17 エラーメッセージ表示ルーチン
 S14 フラッシュROMデータチェックルーチン
 S16 キー入力チェックルーチン
 S18 終了処理&メッセージ表示ルーチン

【図1】



【図2】



【手続補正書】

【提出日】平成9年3月7日

【補正方法】変更

【手続補正1】

【補正内容】

【補正対象書類名】図面

【図2】

【補正対象項目名】図2

